



## Necessity of Teaching Information Security and Cyber-Security in Primary Education

**Mahfuza Gafurova,**

*Doctor of Philosophy (PhD) in Pedagogical Sciences, Fergana State University*

**Yodgoroy Mamatova,**

*Master's Student of Fergana State University, Uzbekistan*

### Abstract

*This article emphasizes the necessity of information security and its impact on primary pupils and problems that have been emerging because of cyber liberty, cyber-crimes, its targets, types that may endanger the children, measures that have been implemented to overcome this problem in our country and overseas, suggests several educational games and methods so as to defend pupils from detrimental informations that should be put into practice, suggestions and recommendations are given for parents and pedagogs.*

### ARTICLE INFO

#### Article history:

Received 3 Apr 2023

Revised form 5 May 2023

Accepted 7 Jun 2023

**Key words:** techno-ethics, information security, cyber-crime, cyber-security, cyber-threat.

© 2023 Hosting by Central Asian Studies. All rights reserved.

\*\*\*

### Introduction

It is not exaggeration to say that education and training have been being enriched with the influence of modern technologies. In this fast paced development, there have been emerging the concepts of educational games based technologies, teaching with the help of didactic games and innovation technologies, integrated educational technologies so as to make it more effective and more intriguing. Those games are accomplished with internet, mobile phones, personal computers and so on. Those modern technologies give wide range of opportunity for students to utilize several networks of information technologies.

This requires the young generation to acquire the necessary knowledge and skills to protect themselves from various information attacks and cyber-threats, to develop immunity against the negative consequences of harmful information, critical thinking, technoethics and cyber-security.

Cyber security is an important issue for us and for the next generation. When the weapon of crime is the Internet and the latest digital technologies, the target can be any person, firm or enterprise, or even the state. Unfortunately, we haven't fully realized it yet! " As we know from the attacks on the Google search engine

that not only governments, but also private companies are victims of this threat. Global economic integration has opened many doors for us, and opportunities for criminals," says Robert Mueller, head of the United States Federal Bureau of Investigation (FBI) [8]. So, this is one of the global problems of our world. As another proof of my opinion, I find it permissible to quote a passage from the speech of former American President Barack Obama. In his opinion, cyber security is one of the most urgent problems of the 21st century. They will never be left behind by nuclear weapons and weapons of mass destruction. In order to fight against computer crime in the United States, the Federal Computer Fraud and Abuse Act of 1996 was adopted and the Federal Bureau of Investigation (FBI) was established to resist this type of crime. Since these years, this country has realized the new threat to the country's security and the power of information weapons, and has been taking necessary measures [8].

In our country, the Constitution of the Republic of Uzbekistan is considered to be the main source of norms regulating relations in the field of information, and many researchers are working in this regard. However, taking into account the fact that children's minds are rapidly growing in sync with time and technology, and as a result, various information attacks have a negative effect on their mental and physical development, it is important to enrich technoethics in the young generation behavior during elementary education. It is necessary to apply measures and conducted research in this regard.

### Materials and Methods

Chapter 15 of the Constitution of the Republic of Uzbekistan is called "Mass media" and the following is stated in this chapter: "The mass media are free and work according to the law.

The state guarantees the freedom of media activity, their rights to seek, receive, use and disseminate information. Mass media are responsible for the reliability of the information they provide."

Also, "Censorship is not allowed. Obstructing or interfering with the activities of the mass media is a cause of liability according to the law" [1].

During our research, we analyzed the benefits and harms of freedom of information for the educational process. In the words of the researcher Schuesster, "On the one hand, information technologies serve to make the work and educational activities of students and teachers faster, more efficient and productive. On the other hand, it is not secret that information threats harm the school and its honor and cause various legal responsibilities and financial losses" [12]. Researchers Whitman and Mattford in their book "Principles of Information Security" said, that : "If we are not aware of hidden cyber-threats, all people, products, and activities can be at risk" [14]. Katzan, in his 2016 article on "Modern issues in cyber security" in the Scientific Research Journal of Information Security, stated that the school is becoming a target of cyber-attacks. He believes that its main reason is inadequacy of unconquerable information security infrastructure that can withstand pervasive information threat of the world [7].

In many countries of the world, there are cyber-attacks causing suspense among school teachers and students. Many foreign researchers believe the following information stored in school databases can be available for cyber criminals:

- personal phone numbers of students and teachers;
- credit cards of school employees;
- medical information;
- names, places of residence of students, parents and teachers;
- their e-mails;
- documents on their achievements;
- exam answers and results;
- time of participation in school clubs and places where clubs are held;
- all school documents and others [9].

One of the most urgent problems of schools is cyber security, and the reason for this is that people are becoming more connected to the Internet and information technologies year by year. Cyber-theft, cyber-crime, and vandalism threaten schools and those who study and work in there. Criminals believe that school is a path that opens up many opportunities: organizing cyber-attacks on people's information in databases, using their phone numbers about winning lotteries, getting housing, cars without credit dets , sending false messages asking for financial help to people with limited low income via school administration , and they are getting a lot of profit through this. Below are the types of cybercrime cases that can be committed at school:

- data breach (illegal personal data breach);
- cases of phishing/skimming (individual financial crimes);
- technological threats (aimed at disabling computer devices);
- cases of spreading unnecessary messages (dissemination of information containing obscenity, violence, racism, and disparaging of various people that disturb the minds of children);
- irritate and bother (cyber-violence, cyber-harassment. This is an example of situations where people are asked to pay money in order not to disclose their confidential personal information)[ 11,26

In addition, based on the research results of the most influential honorable researchers in the field of media, it can be noted that more young people are chosen as objects of manipulation by the mass media, because:

- they do not fully perceive an important part of information, because they are not yet ready to differentiate it;
- they partially understand the meaning of messages or that they can have several meanings;
- they take a passive position towards the mass media, do not know how to protect themselves from their influence and often do not understand the need for such protection[6, 341].

## Results and Discussions

Based on the experience with the students, we witnessed that the above opinions are valid. In order to conduct research on the subject, we selected 27 students of the 4th "A" class of the 43rd general secondary school of the Kurgantepa district of the Andijan region. Through the interview method, we found out their understanding of information security. Through questionnaires, we got the answer to the following questions: what kind of activities do they do in their free time, which technological devices can they use during the day, for what purpose do they mainly use the devices, what information can be harmful and which can be useful.

Although it is considered necessary to know information security for elementary school students nowadays, it is not taught to them as a separate subject. For this reason, we believe that it is necessary to teach primary school students during class hours. For them, it may seem difficult, confusing and boring, so we chose the game method. Before that, explanatory work is carried out with students about harmful information, information security and technoethics, after which the following games can be used:

- "Yes and no" - in this game, students are divided into small groups and group leaders are invited to the board and asked quick questions.

For example:

Questions	Answers
Are computer viruses contagious for people?	No
Do antivirus protect computers?	Yes
Is internet global network?	Yes
Is it necessary to defend personal informations?	Yes
Does virus help to fasten computer programs?	No

- “Claster” method - - this method also comes in handy to drill knowledge effectively. To fulfill this method teacher should draw two circle patterns on the board: writes “Personal data” for the first and “Ordinary data” for the second. Students should fill according to what they learnt. It is recommended to divide the group into two groups.

Through this method, students will learn more fully what information is personal that needs to be protected, and what information is ordinary information that can be disclosed to other people. As a result, they develop

critical thinking and immunity to various types of information.

- "Two-part diary" method - this is done in written form and helps to reinforce concepts and terms related to information security. In this case, the notebook page is divided vertically into two parts. Concepts are given to one part, and information to explain it to another. Students will have to fill in the blanks. Below are the questions that can be asked about the topic:

## RESULTS AND DISCUSSION

The former information shows that in the age of information, the minds of young generations are affected by a huge flow of information. Metaphorically speaking, this is like living under a "rain of information" or a "flood of information".

If we look at the results of the research, only 20% of the students are busy with various tuition activities in their free time. Only 15% of them can express a critical thinking on the messages coming from the information stream. More than 50 percent prefer to watch games, entertainment shows, cartoons, and movies through their own smartphones, and the rest through their parents' phones. Researcher Rahman puts forward the opinion that mass media attracts children whose minds are not yet sufficiently developed, they are not separated from regular information devices, become dependent on them, and lead to addiction [10]. As a result, rudeness, temper tantrums, loss of respect for loved ones are observed in children, and if we look at it physically, the rays of technological devices have a negative effect on the eyes and the whole body, causing serious diseases. , all of this is an "invisible" threat to the developing children's world, cyber-bullying in technologies, attacks on school information systems, cyber-crimes are another threat [13]. The law of the Republic of Uzbekistan "On the protection of children from information that harms their health" shows that our government protects young people from informational threats. Article 5 of it lists the main directions of the state policy in the field of protecting children from harmful information:

The main directions of the state policy in the field of protecting children from information harmful to their health are as follows:

- creation of legal, socio-economic, organizational and technical conditions ensuring protection of children from information harmful to their health, as well as development of scientific and practical research in this field;
- prevention of illegal information-spiritual influence on the minds of children, use of tricks on them, distribution of information products encouraging children to engage in antisocial actions, as well as prevention of offenses in this area;
- supporting the activities of citizens' self-management bodies, non-governmental non-profit organizations, other institutions of civil society, individuals and legal entities in the field of protecting children from information harmful to their health;
- development and improvement of criteria, mechanisms and methods of classification of information harmful to children's health, introduction of software, hardware and technical means of ensuring children's information security [2]. Learning about information security and the ethics of using technological devices is useful for everyone. As a result of the conversation with many young people, I realized that people do not want to spend money, participate in various seminars and study courses to get knowledge about information security. This means that many citizens are unaware of the importance of cyber security and its impact. For this reason, students' moral immunity against harmful information and critical thinking qualities should be taught in schools that are considered to be continuous education. Information security knowledge can be instilled in the minds of children during school hours or in other subjects. For example, in mother tongue and reading classes, short essays and texts can be used under the topics of information threat and protection against it. In addition, the school administration should organize various competitions, seminars, and roundtable discussions in this regard, and teachers should acquire knowledge about information technologies, harmful information, and protection against cyber-attacks, regardless of their specialization, and teach them to students as much as possible. to teach, to carry out consistent work in cooperation with parents in this regard, to explain the urgency of the problem to parents, to ensure that children are under control both at school and at home, and to spend

their free time for the purpose of meaningful organization, it is necessary to create wide conditions for them to engage in group activities based on their interests.

### Conclusion

To sum up, today's rapidly developing information society creates new opportunities for us as well as a number of problems. There is no doubt that the victims of such threats and attacks are often schoolchildren, and its target is the school and its information base. The best way to solve these problems is to counter them with knowledge and to teach children about information threats at a young age, because knowledge is an invincible power! Instead of saying "this threat does not endanger me" and "it doesn't matter to me", we should start taking necessary measures now.

### References:

1. Constitution of the Republic of Uzbekistan. - Tashkent: Uzbekistan, 2020.
2. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan, T, 22.10.2018, No. 848, Article 5
3. Alavi, R., Islam, S., & Mouratidis, H. An information security risk-driven investment model for analyzing human factors// Information and Computer Security, 2016, 24(2). - B. 205-227.
4. Abrorkhonova K. A. The technology of forming the culture of working with information among primary school students// International scientific journal, 2022, Vol 8,2. - B. 2103-2109.
5. Karimov I.M., Turgunov N.A. Fundamentals of information security - Tohkent: Ministry of Internal Affairs of the Republic of Uzbekistan, 2016 - 91 p.
6. Karshiyev B. E. Media education is an important factor in protecting young people from negative information// Academic research in educational sciences, 2021, Vol 2, No. 12. - P. 340-345.
7. Katzan, Jr., H. Contemporary issues in cybersecurity// Journal of Cybersecurity Research, 2016, 1(1). - B. 1-6.
8. Cyber crimes are a new era, a new problem. <https://www.amerikaovozi.com/a/a-36-2010-03-26-voa1-93371769/807021.html> (27.03.2023)
9. McGettrick, A. Toward effective cybersecurity education// IEEE Security & Privacy, 2013. -B. 6(11),-68.
10. Rahman N. A., Sairi I. H. The importance of cybersecurity education in school// International journal of information and education technology, 2020, Vol. 10, No. 5. - P. 378-382.
11. Richardson M. D , Walter E. S, Lemoine P. A., Waller R. E. Planning for cyber security in schools: human factor// Educational planning, 2020, Vol 27, No 2. - P. 23-39.
12. Schuesster, J. H. Contemporary threats and countermeasures// Journal of Information, Privacy & Security, 2013, 9(2). - B. 3-20
13. Yoziye U. L. Improved technology of protecting students from the threat of harmful information in the educational process (in the case of primary education). Doctor of Philosophy in Pedagogical Sciences (PhD)... diss. abstract. - Nukus, 2018. - B.47
14. Whitman M. E., Mattord H. J. Principles of information security// Boston, MA: Cengage Learning, . (5th Ed), 2016.
15. Alijon, A., Xoldorovich, S. Z., & Abbosovna, G. M. kizi, MMA.(2022). Technology of Individualization of Learning. *Spanish Journal of Innovation and Integrity*, 6, 291-297.
16. Gafurova, M. A. (2022). Improving Mental Skills Of Students By Analyzing And Solving Problems. *Current Research Journal Of Pedagogics*, 3(01), 40-44.
17. Gafurova, M. A. (2021). Developing Cognitive Activities of Primary School Students based on an Innovative Approach. *International Journal of Multicultural and Multireligious Understanding*, 8(10), 236-242.
18. Gofurova, M. A. (2020). Development of students' cognitive activity in solving problems. *ISJ Theoretical & Applied Science*, 1(81), 677-681
19. Gofurova, M. A. (2020). Развитие познавательной деятельности учащихся при решении задач. *Theoretical & Applied Science*, (1), 677-681.
20. Gafurova, M. A. (2023). Development of Cognitive Activity of Elementary School Students in Mathematics Lessons. *Global Scientific Review*, 14, 35-39.